3 Feb 22

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

Thousands of Malicious npm Packages Threaten Web Apps

Attackers increasingly are using malicious JavaScript packages to steal data, engage in cryptojacking and unleash botnets, offering a wide supply-chain attack surface for threat actors. New research from open-source security and management firm WhiteSource has discovered the disturbing increase in the delivery of malicious npm packages, which are used as building blocks for web applications.

https://threatpost.com/malicious-npm-packages-web-apps/178137/

Meet Coinstomp: New Cryptojacking Malware Targets Asian Cloud Service Providers

Dubbed CoinStomp, the malware is compromised of shell scripts that "attempt to exploit cloud compute instances hosted by cloud service providers for the purpose of mining cryptocurrency," according to Cado Security. A number of attack attempts have been focused, so far, on cloud service providers in Asia.

https://www.zdnet.com/article/meet-coinstomp-new-cryptojacking-malware-targets-asian-cloud-service-providers/?&web_view=true

KP Snacks Giant Hit by Conti Ransomware, Deliveries Disrupted

KP Snacks, a major producer of popular British snacks has been hit by the Conti ransomware group affecting distribution to leading supermarkets.

https://www.bleepingcomputer.com/news/security/kp-snacks-giant-hit-by-conti-ransomware-deliveries-disrupted/

SEO Poisoning Pushes Malware-Laced Zoom, Teamviewer, Visual Studio Installers

A new SEO poisoning campaign is underway, dropping the Batloader and Atera Agent malware onto the systems of targeted professionals searching for productivity tool downloads, such as Zoom, TeamViewer, and Visual Studio. Poisoning search resultsAs part of this campaign, the threat actors perform search engine optimization (SEO) techniques to legitimate compromised sites into search results for popular applications.

https://www.bleepingcomputer.com/news/security/seo-poisoning-pushes-malware-laced-zoom-teamviewer-visual-studio-installers/

Walmart Dissects New Sugar Ransomware

The cyber threat team at retail giant Walmart has dissected a new ransomware family dubbed Sugar, which is available to cybercriminals as a ransomware-as-a-service (RaaS). The Sugar ransomware family is written in Delphi and borrows objects from other ransomware families out there.

https://www.securityweek.com/walmart-dissects-new-sugar-ransomware

BlackCat Ransomware Implicated in Attack on German Oil Companies

An internal report from the Federal Office for Information Security (BSI) said the BlackCat ransomware group was behind the recent cyberattack on two German oil companies that is affecting hundreds of gas stations across northern Germany. Read MoreGerman newspaper Handelsblatt managed to obtain the internal report that said Oiltanking's "systems were compromised by the BlackCat ransomware through a previously unknown gateway."

https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/#ftag=RSSbaffb68

UEFI Firmware Vulnerabilities Affect at Least 25 Computer Vendors

Researchers from firmware protection company Binarly have discovered critical vulnerabilities in the UEFI firmware from InsydeH2O used by multiple computer vendors such as Fujitsu, Intel, AMD, Lenovo, Dell, ASUS, HP, Siemens, Microsoft, and Acer. UEFI (Unified Extensible Firmware Interface) software is an interface between a device's firmware and the operating system, which handles the booting process, system diagnostics, and repair functions.

https://www.bleepingcomputer.com/news/security/uefi-firmware-vulnerabilities-affect-at-least-25-computer-vendors/

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code ExecutionMS-ISAC ADVISORY NUMBER:2022-017DATE(S) ISSUED:OVERVIEW:Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet.

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2022-017/

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution. MS-ISAC ADVISORY NUMBER:2022-015DATE(S) ISSUED:OVERVIEW:Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for arbitrary code execution.

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2022-015/

Multiple Vulnerabilities in Cisco Products Could Allow for Arbitrary Code Execution

Multiple Vulnerabilities in Cisco Products Could Allow for Arbitrary Code ExecutionMS-ISAC ADVISORY NUMBER:2022-011DATE(S) ISSUED:OVERVIEW:Multiple vulnerabilities have been discovered in Cisco Products, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute code on the affected systems.

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-products-could-allow-for-arbitrary-code-execution_2022-011/